ISSN2519-206X. Researches in Mathematics and Mechanics.–2016.–V.21, Is.1(27).–P.100–108

UDC 511.32+004.421.5

S. Varbanets
I. I. Mechnikov Odesa National University

CIRCULAR GENERATOR OF PRN'S

Let E_m be a subgroup of multiplicative group of reduced residues modulo p^m, $p \equiv 3 \pmod 4$ in the ring of Gaussian integers with norm one $(\mod p^m)$. Using the description of elements from E_m we construct the sequence of real numbers which satisfies the condition of equidistribution and statistical independency, i.e. it is a sequence of PRN's.
MSC: 11K45, 11T23, 11T71.
Key words: pseudorandom numbers, exponential sum, discrepancy.

Introduction. The sequence of real numbers $\{a_n\}$, $0 \leqslant a_n < 1$, we call the sequence of pseudorandom numbers (arbitrary, PRN's) if it is produced by deterministic generator and being a periodical sequence has the statistical properties such that it looks like to implementation of the sequence of random numbers with independent and uniformly distributed values on $[0, 1)$. More acceptable sequences of PRN's generate by the congruential recursion

$$y_{n+1} \equiv f(y_n, y_{n-1}, \dots, y_{n-k+1}) \pmod m, \tag{1}$$

where $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, $f(u_1, \dots, u_k)$ is integer function over $\mathbb{Z}_m^k$.

In case $f \in \mathbb{Z}_m[u_1, \dots, u_k]$ we have the congruential polynomial generator of periodical sequence $\{y)n\}$ with a period τ, $\tau \leqslant m$.

It emerged that linear function $f(u) = au + b$ does not supply requirements of "affinity" to statistical independency (unpredictability) (see, for example [11])

But quadratic function $f(u) = au^2 + bu + c$ satisfies to condition of "practical" unpredictability (see: [8]).

The generator associated with quadratic function $f(c)$ we call parabolical.

The requirements to uniform distribution and unpredictability is satisfied the following inversive generator

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m}, \tag{2}$$

where p is a prime number, $a, b \in \mathbb{Z}$, y_n^{-1} is a multiplicative inverse to $y_n \pmod{p^m}$.

The inversive generator (2) and its generalization was being investigated by many authors (see: [3–10], [14–18]).

Starting out from our reasoning we will call such inversive generator as hyperbolical.

To apply the sequence $\{y_n\}$ in cryptography it is necessary to carry-out the requirement of secrecy as well. That means providing the impossibility to restore the generator parameters by single values of sequence elements. There are some interesting researches about this area (see: [1–4] [9, 10]). In the paper [18] there are being investigated the analogues of inversive congruential generators, that without any increases of computational complexity of finding the elements of sequence $\{y_n\}$, get

Received 25.09.2015

essential complexity for intruder's work around parameters of inversive or linear generator to be recovered.

Let $p \equiv 3 \pmod 4$ be a prime rational number, m be a natural. Denote G the ring of gaussian integers, $G = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\}$, and G_{p^m} (accordingly, $G^*_{p^m}$) the ring of residue classes (accord., multiplicative group of this ring modulo p^m) over G.

Let

$$E_m := \left\{\alpha \in G^*_{p^m} :\ N(\alpha) \equiv \pm 1 \pmod{p^m}\right\}.$$

It easy to check, that E_m is a subgroup in $G^*_{p^n}$ with order $2(p+1)p^{m-1}$, that we call the norm group over the ring G_{p^m}. As far as E_m is a cyclic group, it means that every generated element $u + iv$ defines two sequences of integer numbers modulo p^m:

$$Z_n = \Re((u+iv)^n) \qquad \textit{and} \quad W_n = \Im((u+iv)^n),\ \ n = 1, 2, \ldots.$$

The main point of this work is to prove that the sequences $\left\{\frac{Z_n}{p^m}\right\}$ and $\left\{\frac{W_n}{p^m}\right\}$ are uniformly distributed on $[0, 1)$.

Notation and auxiliary results. Before studying the sequences of PRN's produced by circular generator, we standardize some notations to be used throughout this paper.

Lower case Roman (respectively, Greek) letters usually denote rational (respectively, Gaussian) integers; inparticular, m, n, k are positive integers and p is always a rational prime number $p \equiv 3 \pmod 4$. We also define a *norm* over $\mathbb{Q}(i)$ into $\mathbb{Q}$ by $N(\alpha) = |\alpha|^2$. For the sake of convenience, we denote by G the set of the Gaussian integers. Let $\mathbb{Z}_q$ (or G_q) denotes the ring of residue classes modulo q, and $\mathbb{Z}^*_q$ (or G^*_q) denotes the multiplicative group in $\mathbb{Z}$ (or G_q). If $x \in G^*_q$ we write x^{-1} for the multiplicative inverse of x mod q, i.e. x^{-1} is an arbitrary Gaussian integer sutysfying the condition $xx^{-1} \equiv 1 \pmod q$. As usual, $gcd(a, b)$ or (a, b) stand for the greater common divisor of a and b (or, respectively, α and β in G), Through $\mathbb{Z}[x]$ (or $G[x]$) we denote the polynomial ring over $\mathbb{Z}$ (or G). For $a \in \mathbb{Z}$ ($\alpha \in G$) stand $\nu_p(a)$ (or $\nu_p(\alpha)$) if $p^{\nu(a)} | a$, $p^{\nu(a)+1} \nmid a$.

Before starting out the study of the sequences $\{Z_n\}$ and $\{W_n\}$ we need several lemmas being used in sequel.

Lemma 1. *Let $f(\xi) = \alpha_1\xi + \alpha_2\xi^2\mathfrak{p} + \alpha_3\xi^3\mathfrak{p}^{\nu_3} + \cdots + \alpha_k\xi^k\nu_{\mathfrak{k}}$, where $\nu_3, \nu_4, \ldots, \nu_k$, $n \geqslant 2$ be positive integers, $\alpha_1, \ldots, \alpha_k \in G$, $(\alpha_2, \mathfrak{p}) = \cdots = (\alpha_k, \mathfrak{p}) = 1$. Then we have*

$$|S(f, \mathfrak{p}^n)| \leqslant \begin{cases} 0 & if \quad \mathfrak{p} \neq 1+i,\ (\alpha_1, \mathfrak{p}) = 1 \\ & or \quad \mathfrak{p} = 1+i,\ \alpha_1 \not\equiv 0 \pmod{\mathfrak{p}^2}, \\ N(\mathfrak{p})^{\frac{n+1}{2}} & if \quad \mathfrak{p} \neq 1+i,\ \alpha_1 \equiv 0 \pmod{\mathfrak{p}}, \\ 2^{\frac{n+3}{2}} & if \quad \mathfrak{p} = 1+i,\ \alpha_1 \equiv 0 \pmod 2. \end{cases}$$

Proof. For $n = 2$ the estimated sum is the Gaussian sun, and thus in such case our assertion holds.

For $n \geqslant 3$, $\mathfrak{p}$ be a odd prime. We put

$$\xi = \eta + \mathfrak{p}^{n-1}\zeta,\ \ \eta \in G_{\mathfrak{p}^{n-1}},\ \ \zeta \in G_{\mathfrak{p}}.$$

Taking into account that $\xi^k = \eta^k + k\eta^{k-1}\zeta \pmod{\mathfrak{p}^{n-1}}$, we get

$$S(f,\mathfrak{p}^n) = \sum_{\eta \in G_{\mathfrak{p}^{n-1}}} e^{2\pi i \Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right)\Re\left(\frac{\alpha_1+2\alpha_2\eta}{\mathfrak{p}}\zeta\right)} = N(\mathfrak{p}) \sum_{\substack{\eta \in G_{\mathfrak{p}^{n-1}} \\ \alpha_1+2\alpha_2\eta \not\equiv 0 \pmod{\mathfrak{p}}}} e^{2\pi i \Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right)}.$$

Let $\alpha_1 + 2\alpha_2\eta_0 \equiv 0 \pmod{\mathfrak{p}}$, $\eta_0 \in G^*_{\mathfrak{p}}$. We put $\eta = \eta_0 + \mathfrak{p}\xi$, $\xi \in G_{\mathfrak{p}^{n-2}}$. Then we infer

$$f(\eta_0 + \mathfrak{p}\xi) = f(\eta_0) + \mathfrak{p}(\alpha_1 + 2\alpha_2\eta_0)\xi + \mathfrak{p}^2\alpha_2'\xi^2 + \cdots = f(\eta_0) + \mathfrak{p}^2 f_1(\xi),$$

where the polynomial $f_1(\xi)$ has such type as $f(\xi)$.

So, after $\left[\frac{n}{2}\right]$ steps we obtain

$$|S(f,\mathfrak{p}^n)| = \begin{cases} N(\mathfrak{p})^{\frac{n}{2}} & if \quad n \text{ is even}, \\ N(\mathfrak{p})^{\frac{n-1}{2}} \left| \sum\limits_{\xi \in G_{\mathfrak{p}}} e^{2\pi i \Re\left(\frac{\beta_1+\beta\xi^2}{\mathfrak{p}}\right)} \right| & if \quad n \text{ is odd}. \end{cases}$$

By the estimate of the Gauss sum we have the assertion of Lemma.

The case $\mathfrak{p} = 1 + i$ can be considered similarly. ■

Corollary 1. *Let $f(\xi) = \alpha\xi + \beta\xi^2 + \mathfrak{p}(\gamma\xi^2 + \cdots)$ be a polynomial over G, and let $(\beta, \mathfrak{p}) = 1$. Then for any $\delta \in G$, we have*

$$\left| \sum_{\xi \in G^*_{\mathfrak{p}^n}} e^{2\pi i \Re\left(\frac{f(\xi)+\delta\xi^{-1}}{\mathfrak{p}^n}\right)} \right| \leqslant 2N(\mathfrak{p})^{\frac{n}{2}}.$$

Indeed, putting $\xi = \eta + \mathfrak{p}^{n-1}\zeta$, $\eta \in G^*_{\mathfrak{p}^{n-1}}$, $\zeta \in G_{\mathfrak{p}}$, and observing that $\xi^{-1} = \eta^{-1} - \mathfrak{p}^{n-1}\xi(\eta^{-1})^2$, where η^{-1} be a multiplicative inverse mod$\mathfrak{p}^n$ for η, we immediately infer that inequality holds by Lemma 1.

Similarly, assertion holds for the same exponential sums over $\mathbb{Z}_{p^n}$.

Let us denote by E_m the following subgroup of $G^*_{p^m}$, $p \equiv 3 \pmod 4$, p be a prime number in $\mathbb{Z}$:

$$E^+_m := \{x \in G^*_{p^m} \ : \ N(x) \equiv 1 \pmod{p^m}\}.$$

The subgroup E^+_m we will call the norm group in $G^*_{p^m}$.

Take into account that the multiplicative group of the field G_p is a cyclic group. It is easy to prove (as in $\mathbb{Z}^*_{p^m}$) that it exists a generating element of the group E^+_1, such that it will generate every group E^+_m, $m > 1$.

In order to find that element, we take such generating element g_0 of group G^*_p for which $g_0^{(p+1)p} = 1 + hp^2$ with $(h,p) = 1$. Then g_0^{p-1} is revealed generating element of group E^+_m, $m = 1, 2, \ldots$.

Moreover, we have

Lemma 2. *Let us $u+iv \in E_m$ be a generating element of E_m. Then $ord(u+iv) = |E_m| = 2(p+1)p^{m-1}$ and*

$$(u+iv)^{2(p+1)} = 1 + p^2x_0 + ipy_0,$$
$$x_0 + 2y_0^2 \equiv 0 \pmod p, \ (x_0, p) = (y_0, p) = 1,$$

and also for any $t = 4, 5, \ldots$, *we have modulo* p^m

$$\begin{aligned} \Re(u+iv)^{2(p+1)t} &= A_0 + A_1 t + A_2 t^2 + \cdots + A_{m-1} t^{m-1}, \\ \Im(u+iv)^{2(p+1)t} &= B_0 + A_1 t + B_2 t^2 + \cdots + B_{m-1} t^{m-1}, \end{aligned} \tag{3}$$

where

$$\begin{cases} A_0 \equiv 1 \pmod{p^4},\ B_0 \equiv 0 \pmod{p^4}, \\ A_1 \equiv p^2 x_0 + \frac{1}{2} p^2 y_0^2 \equiv 0 \pmod{p^3},\ B_1 \equiv p y_0 \pmod{p^3}, \\ A_2 \equiv -\frac{1}{2} p^2 y_0^2 \pmod{p^3},\ B_2 \equiv 0 \pmod{p^3}, \\ A_j \equiv B_j \equiv 0 \pmod{p^3},\ j = 3, 4, \ldots m-1. \end{cases} \tag{4}$$

Denote

$$\begin{aligned} (u+iv)^{2k} &= u(k) + iv(k),\ 0 \leqslant k \leqslant p, \\ (u+iv)^{2(p+1)t+2k} &\equiv \sum_{j=0}^{m-1} \left(A_j(k) + iB_j(k)\right) t^j \pmod{p^m}. \end{aligned}$$

It is clear

$$\begin{aligned} A_j(k) &= A_j u(k) - B_j v(k), \\ B_j(k) &= A_j v(k) + B_j u(k). \end{aligned}$$

Thus from Lemma 1 we have

Corollary 2. *For* $k = 1, 2, \ldots, p$, *we have*

$$\begin{aligned} & u(k) \equiv u(-k),\ v(k) \equiv -v(-k) \pmod{p^m}, \\ & (u(k), p) = (v(k), p) = 1,\ if\ k \neq \frac{p+1}{2}, \\ & u(0) = 1,\ v(0) = 0, \\ & u(k) \equiv 0 \pmod{p},\ (v(k), p) = 1,\ if\ k = \frac{p+1}{2}. \end{aligned}$$

Moreover, for $k \neq \frac{p+1}{2}$

$$\begin{aligned} & A_0(k) \equiv u(k),\ B_0(k) \equiv v(k) \pmod{p}, \\ & p || A_1(k),\ p || B_1(k),\ p^2 || A_2(k),\ p^2 || B_2(k); \end{aligned}$$

and

$$\begin{aligned} & A_1(0) \equiv 0 \pmod{p^4},\ B_1(0) \equiv p y_0 \pmod{p^4},\ p^2 || A_2(0),\ B_2(0) \equiv 0 \pmod{p^3}, \\ & A_0(k) \equiv 0,\ B_0(k) \equiv 0 \pmod{p}, \\ & P || A_1(k),\ p^2 || B_1(k),\ p^2 || A_2(k),\ B_2(k) \equiv 0 \pmod{p^3}\ if\ k = \frac{p+1}{2}, \\ & A_j(k) \equiv B_j(k) \equiv 0 \pmod{p^3},\ k = 0, 1, \ldots, p,\ j \geqslant 3. \end{aligned}$$

The proof of Corollary is a simple exercise (in view the congruence

$$\begin{aligned} & (u+iv)^{p+1} = 1 + p^2 x_0 + i y_0, \\ & (x_0, p) = (y_0, p) = 1, \\ & 2x_0 + y_0^2 \equiv 0 \pmod{p}, \\ & u^2 + v^2 \equiv +1 \pmod{p^m} \qquad), \end{aligned}$$

and we omit.

Main Results

1. Circular generator of PRN's. We select a random number k from $\{0, 1, 2, \dots, p-1\}$ and consider the sequence $\{(u+iv)^{2(p+1)t+2k}\}$, $t = 0, 1, \dots, p^{m-1}-1$, where $u+iv$ is a generating element of E_m.

Denote

$$Z_t(k) = Z_t = \Re\Big((u+iv)^{2(p+1)t+2k}\Big),$$
$$W_t(k) = W_t = \Im\Big((u+iv)^{2(p+1)t+2k}\Big).$$

These sequences discribed in Lemma 2.

We saw that $(u+iv)^{2(p+1)} = u_0 + iv_0$, where $u_0 = 1 + p^2x_0$, $v_0 = y_0$, $(x_0, p) = (y_0, p) = 1$ and $x_0 + 2y_0^2 \equiv 0 \pmod p$.

Hence,

$$\begin{aligned} Z_{t+1} &\equiv \Re\big((u_0+iv_0)^t \cdot (u_0+iv_0)\cdot(u(k)+iv(k))\big) \equiv \\ &\equiv Z_t u_0 - W_t v_0 \pmod{p^m}, \end{aligned} \tag{5}$$

$$W_{t+1} \equiv Z_t v_0 + W_t u_0 \pmod{p^m} \tag{6}$$

for $t = 0, 1, \dots, p^{m-1}-1$.

The sequence (5) and (6) satisfies that condition

$$Z_t^2 + W_t^2 \equiv 1 \pmod{p^n}$$

for any $t \in \mathbb{Z}_{p^{n-1}}$ and $k \in \{0, 1, \dots, p\}$.

Thus we call the sequences (5) and (6) circular sequences of PRN's.

Theorem 1. *Let $a, b \in \mathbb{Z}_{p^m}$, $(a, b, p) = 1$. Then for the exponential sum*

$$S(a, b; p^m) = \sum_{t \in \mathbb{Z}_{p^{m-1}}} e_{p^m}(aZ_t + bW_t)$$

we have the following bound

$$|S(a, b; p^m)| \leqslant 2p^{\frac{m}{2}}. \tag{7}$$

Proof. Lemma 2 and its Corollary give

$$aZ_t(k) + bW_t(k) \equiv c_0 + c_1 t + c_2 t^2 + \cdots \pmod{p^m},$$

where notationally of Lemma 2 we have

$$c_j(k) = au_0 A_j(k) - bv_0 B_j(k),\ j = 0, 1, 2, \dots.$$

In particular, taking into account $u_0 = 1 + p^2x_0$, $v_0 = py_0$, we have

$$\begin{cases} c_1 \equiv py_0(-av(k) + bu(k)) + p^2y_0^2(-au(k) - bv(k)) \pmod{p^3}, \\ c_2 \equiv -\frac{1}{2}p^2y_0^2 a \pmod{p^3},\ c_j \equiv 0 \pmod{p^3},\ j \geqslant 3. \end{cases} \tag{8}$$

Therefore, by Lemma 1, we easy obtain

$$|S(a, b; p^m)| \leqslant \begin{cases} 2p^{\frac{m}{2}} & if \quad au(k) - bv(k) \equiv 0 \pmod p \\ 0 & else. \end{cases}$$

■

Corollary. For $1 < T < p^{m-1}$ and any $k \in \{0, 1, \dots, p\}$

$$\left| \sum_{t=0}^{T-1} e^{2\pi i \frac{aZ_t(k)+bW_t(k)}{p^m}} \right| \leqslant 2p^{\frac{m}{2}} \log p^m. \tag{9}$$

Indeed, the inequality (9) is consequence of well-known estimate of incomplete sum by complete sum. ■

Denote

$$aZ_t(k) + bW_t(k) = x_t(a, b; k) := x(t). \tag{10}$$

Theorem 2. *Let s be positive integer, $h_1, \dots, h_s \in \mathbb{Z}_{p^m}$, $(h_1, \dots, h_s, p) = 1$. Then for $s \in \{1, 2, \dots, p-1\}$ the following estimate*

$$S(h_1, \dots, h_s) = \sum_{t=0}^{p^{m-1}-1} e_{p^m}(h_1 x(t) + h_2 x(t+1) + \dots + h_s x(t+s-1)) \ll p^{\frac{m}{2}}$$

holds.
(with an absolute constant depending only on s).

Proof. Using (8) and calculating coefficients for t and t^2 in presentation $h_1x(t) + h_2x(t+1) + \dots + h_sx(t+s-1)$ as a polynomial of t or $(t+1)$,..., or $t+s-1$, we obtain (by Lemma 1) that $S(h_1, \dots, h_s) = 0$ only if $-av(k) + bu(k) \equiv 0 \pmod p$. In such case we estimate the sum $S(h_1, \dots, h_s)$ as $O\left(p^{\frac{m}{2}}\right)$ with the absolute constant in symbol "O". In other cases this sum is zero. ■

Remark 1. *It easy to prove that for the congruence $av(k) \equiv bu(k) \pmod p$ at most six solutions satisfies.*

Corollary. In the conditions of Theorem 2 we have

$$\sum_{t=0}^{T-1} e_{p^m}(h_1 x(t) + h_2 x(t+1) + \dots h_s x(t+s-1)) \ll p^{\frac{m}{2}} \log p^m.$$

2. Discrepancy bound. Consider the sequence $\{x(t)\}$, $t = 0, 1, 2, \dots$ of the elements of $\mathbb{Z}_{p^m}$ defined in (10). Let $\{y(t)\}$ be a sequence of PRN's in interval $[0, 1)$ obtained by the normalization $y(t) = \frac{x(t)}{p^m}$,

The sequence $\{y(t)\}$, $t = 0, 1, \dots$, is purely periodic with the period length $\tau = p^{m-1}$.

Equidistribution and statistical independency properties of pseudorandom numbers can be analyzed based on the discrepancy of certain point sets in $[0, 1)^s$.

Besides the discrepancy, there exist other important criteria for the uniformity and independence of PRN's. We will restrict our attention to the discrepancy, since it is the most important measure of uniformity and independence in connection with PRN's.

For N arbitrary points, $x_0, x_1, \dots, x_{N-1} \in [0, 1)^d$, the discrepancy is defined by

$$D_N(x_0, x_1, \dots, x_{N-1}) = \sup_{I \subset [0,1)^d} \left| \frac{A_N(I)}{N} - |I| \right|, \tag{11}$$

where the supremum is extended over all subintervals I of $[0,1)^d$, $A_N(I)$ is the number of points among $x_0, x_1, \dots, x_{N-1}$ falling into I, and $|I|$ denotes the d-dimensional volume of I.

Our goal is to obtain a nontrivial discrepancy estimate for a part of period for the circular generators of pseudorandom numbers. In particular, we shall estimate discrepancy for the sequence $\{\omega_\ell\}$, $\omega_\ell = \frac{x_\ell}{p^m}$, $\ell \geqslant 0$ and for the sequence $\{\Omega_\ell\}$, $\Omega_\ell = (\omega_\ell, \omega_{\ell+1}, \dots, \omega_{\ell+s-1})$, $\ell \geqslant 0$, $s \geqslant 2$. Well-known that a small value $D(\omega_0, \omega_1, \dots, \omega_{N-1})$ guarantees an uniform distribution $\{\omega_\ell\}$, $\ell \geqslant 0$ on $[0,1)$, and a small value $D(\Omega_0, \Omega_1, \dots, \Omega_{N-1})$ means that the sequence $\{\omega_\ell\}$, $\ell \geqslant 0$, pass the two-dimensional serial test on the statistical independence properties of this sequence. In the cryptographical applications the property of statistical independence means that the circulate congruential pseudorandom sequence $\{x_\ell\}$, $\ell \geqslant 0$, is unpredictable.

In the following, some further notation is necessary.

For integers $d \geqslant 1$ and $q \geqslant 2$, let $C_d(q)$ be the set of all nonzero lattice points $\mathbf{h} = (h_1, \dots, h_d) \in \mathbb{Z}^d$ with $-\frac{q}{2} < h_j \leqslant \frac{q}{2}$ for $1 \leqslant j \leqslant d$. Define for $\mathbf{h} \in C_d(q)$

$$\begin{aligned} r(h,q) &= \begin{cases} 1 & if\ h = 0, \\ q \sin\left(\pi \frac{|h|}{q}\right) & if\ h \neq 0, \end{cases} \\ r(\mathbf{h},q) &= \prod_{j=1}^{d} r(h_j, q) \end{aligned} \tag{12}$$

Moreover, several auxiliary results are given.

Lemma 3. *Let $N \geqslant 1$ and $q \geqslant 2$ be integers. Suppose that $\mathbf{y_0}, \mathbf{y_1}, \dots, \mathbf{y_{N-1}} \in \mathbb{Z}_q^d$. Then the discrepancy of the points $\mathbf{t}_\ell = \frac{\mathbf{y}_\ell}{q} \in [0,1)^d$, $\ell = 0, 1, \dots, N-1$, satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \leqslant \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \frac{1}{r(\mathbf{h}, q)} \left| \sum_{\ell=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_\ell) \right| \tag{13}$$

(Proof see in [13], Theorem 3.1).

Lemma 4. *Let T be the period of the sequence $\{\mathbf{y_k}\}$, $T \geqslant N \geqslant 1$ and $q \geqslant 2$ be integers, $\mathbf{y_k} \in \{0, 1, \dots, q-1\}^d$ for $k = 0, 1, \dots, N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^d$. Then*

$$\begin{aligned} D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \leqslant \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h}, q) r(h_0, T)} \times \\ \times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right| \end{aligned} \tag{14}$$

This assertion follows from Lemma 3 and from an estimate of uncomplete exponential sum through complete exponential sum.

Now it easy to prove the following theorems.

Theorem 3. *Let $p \equiv 3 \pmod 4$ be a prime number and let $x(k,\ell) := x(\ell) = a\Re\big((u+iv)^{2(p+1)\ell+2k}\big) + b\Im\big((u+iv)^{2(p+1)\ell+2k}\big)$ be the sequence circular PRN's. Then*

for any $k \in \{0, 1, \ldots, p\}$, $k \neq \frac{p+1}{2}$ *we have*

$$D_N\left(\frac{x(0)}{p^m}, \frac{x(1)}{p^m}, \ldots, \frac{x(N-1)}{p^m}\right) \leqslant \frac{1}{p^m} + \frac{2p^{\frac{m}{2}}}{N}\left(\frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^2 + 1\right),$$

where $1 \leqslant N \leqslant p^{m-1} - 1$.

Theorem 4. *Let* $\mathbf{t}_\ell$, $\ell = \{0, 1, \ldots, p^{m-1} - 1\}$ *be a sequence of points* $\mathbf{t}_\ell \in [0, 1)^s$, $\mathbf{t}_\ell = (x(\ell), x(\ell+1), \ldots, x(\ell+s-1))$. *Then the following estimate for* $T = p^{m-1}$ *and* $s \leqslant p - 1$

$$D_T^{(s)} := D_T(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{T-1}}) \leqslant \frac{s}{p^m} + \frac{1}{p^{\frac{m-1}{2}}}\left(1 + \frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^s\right).$$

holds.

The proofs of these theorems follow from the estimates of theorems 1 and 2 and their corollaries.

From Theorem 3 and 4 it follows that the sequences $\{\Re\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ and $\{\Im\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ are equidistributed and pass s-dimensional test on unpredictability.

Conclusion. Using the description of elements from E_m we construct the sequence of real numbers which satisfies the condition of equidistribution and statistical independency, i.e. it is a sequence of PRN's.

1. **Blackburn S. R.** Predicting nonlinear pseudorandom number generators / S. R. Blackburn, D. Gomez-Peres, I. Gutierrez, I. Shparlinski // Math. Comp. – 2004. – 74(251). – P. 1471–1494.
2. **Blackburn S. R.** Reconstructing noisy polynomial evaluation in residue rings / S. R. Blackburn, D. Gomez-Peres, I. Gutierrez, I. Shparlinski // J. of Algorithm. – 2006. – 61(2). – P. 47–59.
3. **Eichenauer-Herrmann J.** Inversive congruential pseudorandom numbers: a tutorial / J. Eichenauer-Herrmann // Internat. Statist. Rev. – 1992. – 60. – P. 167–176.
4. **Eichenauer-Herrmann J.** Pseudorandom number generation by nonlinear methods / J. Eichenauer-Herrmann // Internat. Statist. Rev. – 1995. – 63. – P. 247–255.
5. **Eichenauer-Herrmann J.** A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus / J. Eichenauer-Herrmann, H. Grothe // ACM Transactions of Modelling and Computer Simulation. – 1992. – 2(1). – P. 1–11.
6. **Eichenauer J.** A non-linear congruential pseudorandom number generator / J. Eichenauer, J. Lehn // Statist. Hefte. – 1986. – 27. – P. 315–326.
7. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus / J. Eichenauer, J. Lehn, A. Topuzoğlu // Math. Comp. – 1988. – 51. – P. 757–759.
8. **Eichenauer-Herrmann J.** A survey of quadratic and inversive congruential pseudorandom numbers, in: Monte Carlo and Quasi-Monte Carlo Methods, 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist / J. Eichenauer-Herrmann, E. Herrmann, S. Wegenkittl. – New York: Springer. – 1998. – 127. – P. 66–97.

9. **Eichenauer-Herrmann J.** On the period of congruential pseudorandom number sequences generated by inversions / J. Eichenauer-Herrmann, A. Topuzoğlu // J. Comput. AP. Math. – 1990. – 31. – P. 87–96.

10. **Kato T.** On a nonlinear congruential pseudorandom number generator / T. Kato, L.-M. Wu, N. Yanagihara // Math. of Comp. – 1996. – 65(213). – P. 227–233.

11. **Knuth D. E.** The Art of Computer Programming, Vol. 2:Seminumerical algorithms / Knuth D. E.. – Addison-Wesley, 1998. — 784 p.

12. **Niederreiter H.** Nonlinear methods for pseudorandom number and vector generation / H. Niederreiter // Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems. – Berlin: Springer. – 1992. – 374. – P. 145–153.

13. **Niederreiter H.** Random Number Generation and Quasi-Monte Carlo Methods. SIAM / Niederreiter H. – Philadelphia : Pa., 1992. — 241 p.

14. **Niederreiter H.** Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus / H. Niederreiter, I. Shparlinski // Acta Arith. – 2000. – 90(1). – P. 89–98.

15. **Varbanets S.** Exponential sums on the sequences of inversive congruential pseudorandom numbers / S. Varbanets // Šiauliai Math. Semin.. – 2008. – 3(11). – P. 247–261.

16. **Varbanets S.** On inversive congruential generator for pseudorandom numbers with prime power modulus / S. Varbanets // Annales Univ. Sci. Budapest, Sect. Comp.. – 2008. – 29. – P. 277–296.

17. **Varbanets P.** Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus / P. Varbanets, S. Varbanets // VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine, September 22-28. – 2008. – 4(1). – P. 112–130.

18. **Varbanets S.** Generalizations of Inversive Congruential Generator / S. Varbanets // Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 Septembre 2011. – 2012. – P. 265–282.

Варбанець С. П.
Циркулярний генератор ПВЧ

Резюме

Нехай E_m — підгрупа мультиплікативної групи зведених залишків за модулем p^m, $p \equiv 3 \pmod 4$ в кільці цілих гаусових чисел норми 1 за модулем $\pmod{p^m}$. Користуючись описом елементів із E_m, ми будуємо послідовність дійсних чисел, яка задовільняє умовам рівнорозподіленості та статистичної незалежності, тобто вона є послідовністю ПВЧ.
Ключові слова: псевдовипадкові числа, тригонометричні суми, дискрипансія.

Варбанец С. П.
Циркулярный генератор ПСЧ

Резюме

Пусть E_m есть подгруппа мультипликативной группы приведенных вычетов по модулю p^m, $p \equiv 3 \pmod 4$ в кольце целых гаусовых чисел нормы 1 по модулю $\pmod{p^m}$. Пользуясь описанием элементов из E_m, мы строим последовательность действительных чисел, которая удовлетворяет условиям равнораспределенности и статистической независимости, то есть она является последовательностью ПСЧ.
Ключевые слова: псевдослучайные числа, тригонометрические суммы, дескрипансия.